ABSTRACT

A system and method are provided for monitoring data packets received at a target system. The data packets may be monitored at any layer of the communication protocol to characterize the type of network traffic being sent from a source machine. Upon detection of suspected and/or confirmed attacks on the target system, the monitoring server may block and/or contain data packets associated with the attacking source to prevent continued attacks on the target system. The monitoring server may monitor data packets transparently in approximately in real-time so that users of the system do not experience messaging delays.